Une Solution d'Authentification Unifiée dans un réseau hétérogène

Arnaud Antonelli
Département d'Enseignement en Informatique
Arnaud.Antonelli@uhp-nancy.fr

Samson Bisaro
ESIAL (Ecole Supérieure d'Informatique et Applications de Lorraine)
Samson.Bisaro@uhp-nancy.fr

Christian Maillard
Faculté des Sciences
Christian.Maillard@uhp-nancy.fr

Campus Victor Grignard BP 239 54506 Vandoeuvre-les-Nancy Cedex

Résumé

L'authentification unique « rêve ou réalité »… Qui n'a pas rêvé de conquérir ce Saint Graal… Qui n'a pas, depuis l'avènement des deux mondes Windows et Unix, essayé de centraliser la gestion des comptes afin d'améliorer l'accès des utilisateurs et afin de faciliter l'administration par les ingénieurs systèmes.

Nous avons tous testé les serveurs Windows NT et Windows 2000 pour unifier les environnements Microsoft, le protocole NIS pour unifier les environnements Unix et nous avons tous essayé d'unifier ces deux mondes opposés à coup de Samba, de LDAP, de Kerberos, de pGina… Mais la dure réalité du terrain montre que si un certain nombre de solutions fonctionnent, il est impossible de conserver toutes les fonctionnalités offertes par chacun des environnements si on privilégie un annuaire OpenLDAP unique ou un annuaire Active Directory.

Dans notre cas, nous avons besoin de toutes les fonctionnalités offertes par les deux environnements.

*Après avoir testé plusieurs solutions, nous avons fait le choix d'avoir un Active Directory unique pour l'ensemble de l'Université afin de ne gérer qu'un seul annuaire d'authentification pour les postes Windows (actuellement le réseau comporte **19** serveurs, **850** postes de travail pour 17000 étudiants) et nous avons un annuaire OpenLDAP pour l'authentification Unix et l'authentification des applications web.*

Parallèlement à ce choix, nous avons développé une kyrielle de programmes pour assurer la création et la gestion de ces comptes tant sur le serveur OpenLDAP que sur le serveur Active Directory.

Pour uniformiser les mots de passe, nous avons développé une interface web que les étudiants doivent obligatoirement utiliser pour valider leurs comptes ou pour modifier leurs mots de passe.

L'étudiant dispose donc d'un compte virtuel unique (sésame) pour accéder à la totalité des moyens informatiques mis à disposition par l'Université. Ce n'est pas encore le Graal tel que nous l'avions espéré mais cette solution qui est en production depuis plus d'un an, nous donne l'impression d'avoir presque atteint notre rêve.

Mots clefs

Authentification, MySQL, OpenLDAP, PHP, Apache, IMP, *Active Directory*, Apogée

1 Introduction

En 2000, tous les services d'enseignement des composantes de notre Université, s'occupaient de la création et de la gestion de leurs comptes étudiants. Un étudiant disposait de plusieurs comptes différents sur un même site géographique. Notre Université compte 12 composantes sur 12 sites géographiques répartis dans cinq villes et 3 départements.

Afin de régler ce problème, il a été décidé de tendre vers une solution globale et unique d'authentification. Chaque étudiant doit pouvoir disposer d'un identifiant et d'un mot de passe unique pour accéder à l'ensemble des ressources de l'Université.

Ce document présente de façon chronologique l'avancement du projet et surtout, les différents choix stratégiques et techniques qui ont conduit à la solution actuelle.

L'ensemble des informaticiens de l'Université a été sollicité pour participer à cette aventure car la réussite d'un tel projet ne peut aboutir que s'il reçoit l'aval de tous. Des réunions régulières ont été mises en place pour décider des orientations à suivre en tenant compte des spécificités de chacun.

Notre première volonté a été de n'utiliser exclusivement que du logiciel libre pour réaliser les différents développements nécessaires à la réalisation du projet.

2 La gestion des logins

2.1 Introduction

Dans la première étape du projet, en l'absence de solution simple de centralisation des comptes étudiants et surtout devant la complexité géographique de notre Université, nous nous sommes fixés comme premier objectif de fournir un identifiant unique ainsi qu'une adresse électronique centralisée (Etumail) qui caractérisent l'étudiant dans l'Etablissement.

Il est important de préciser qu'à cette époque, un étudiant dispose de plusieurs logins différents et qu'il dispose aussi de plusieurs adresses électroniques différentes en fonction du nombre de services où il suit ses enseignements. Il était donc nécessaire de commencer à unifier et centraliser ces informations.

Nous avons donc mis en place un système qui permet la création d'un identifiant et d'une adresse électronique uniques pour chaque étudiant afin de pouvoir fournir aux administrateurs systèmes les informations nécessaires à la création de leurs comptes. Ces informations permettent aussi la mise à jour du système de messagerie (Etumail).

Un étudiant peut ainsi disposer d'un même login sur tous ces comptes.

2.2 Les choix techniques

Pour obtenir les informations concernant les étudiants, Apogée était l'outil idéal. Cependant, la base Apogée nous était difficilement accessible et ne pouvait pas aisément contenir les informations que nous avions besoin de générer. En effet, à cette époque, la priorité des informaticiens de gestion était la maîtrise de cet outil récent et la formation des utilisateurs. Leur disponibilité était limitée. Une extraction automatique de la base Apogée était la solution simple pour disposer des informations souhaitées.

Nous avons donc développé notre propre base de données (LOGIN) afin de disposer de la flexibilité nécessaire à notre projet. Nous avons choisi de travailler sur une base MySQL avec des scripts d'accès en PHP.

Pour l'alimentation de notre base de données, nous avons opté pour les fonctionnalités suivantes :

- L'extraction journalière de certains champs d'Apogée afin de générer les nouveaux comptes ainsi que les modifications de comptes.
- La possibilité par un ajout manuel de générer les paramètres d'un étudiant qui n'est pas encore inscrit.
- La mise à jour des paramètres d'un compte en ajout manuel, lorsque l'étudiant s'inscrit.

L'interaction entre les administrateurs systèmes et la base LOGIN s'effectue par le biais de pages web sur un serveur Apache.

Tout le code est commenté au format PHPDoc ce qui nous permet de générer automatiquement la documentation technique en ligne pour les développeurs.

2.3 La base de données

La base de données LOGIN contient plusieurs tables qui permettent de référencer les éléments nécessaires aux administrateurs systèmes et aux applications réseaux présentes ou à venir. Nous avons décidé de baser nos solutions techniques sur cette base de données qui ne sert qu'à être enrichie et consultée.

Initialement les tables principales étaient les suivantes :

- Login : contient toutes les informations concernant les étudiants.
- UFR : liste des UFR et écoles associées à l'UHP.
- Formation : liste des formations offertes par les UFR et écoles.

Nous avons récemment rajouté une nouvelle table qui recense les inscriptions secondaires des étudiants. Cette table va nous permettre de gérer les inscriptions multiples..

2.4 Le peuplement des tables

La base de données est peuplée et mise à jour toutes les nuits afin de refléter au mieux la situation des étudiants de l'UHP. Pour se faire, nous recevons des extractions de la base Apogée, nous isolons et traitons les informations qui nous intéressent puis nous générons celles qui nous manquent. Parmi ces champs générés, nous pouvons citer les éléments suivants :

- Le login constitué des 5 premières lettres du nom de famille et d'un indice.
- L'alias de messagerie sous la forme Prenom.Nom.Indice.
- La provenance de la ligne (Apogée ou Nom du gestionnaire ayant crée l'entrée dans le cas d'un ajout manuel).
- Le champ date_db qui contient la date de la dernière mise à jour de la ligne.

Remarque : L'indice du login et de l'alias de messagerie n'est pas forcément le même. L'indice dans l'alias de messagerie nous permet de régler les problèmes liés aux homonymes (aucun étudiant ne peut avoir une adresse de messagerie de la forme Prenom.Nom)

Parallèlement au peuplement quotidien de la base, il est possible aux administrateurs système de créer des ajouts manuels dans la base de données.

Ce type d'ajout que nous essayons de limiter, est dû au fait que les étudiants ne sont pas forcément tous inscrits dès la rentrée et permet également de régler des cas particuliers (diplômes conjoints avec d'autres universités

par exemple). Dans ce cas de figure, les gestionnaires utilisent une interface web et renseignent le nom, le prénom et la date de naissance des étudiants qu'ils souhaitent ajouter manuellement à la base de données.

Lorsque l'étudiant s'inscrira officiellement à l'université et qu'il apparaîtra dans Apogée, la ligne sera mise à jour et complétée.

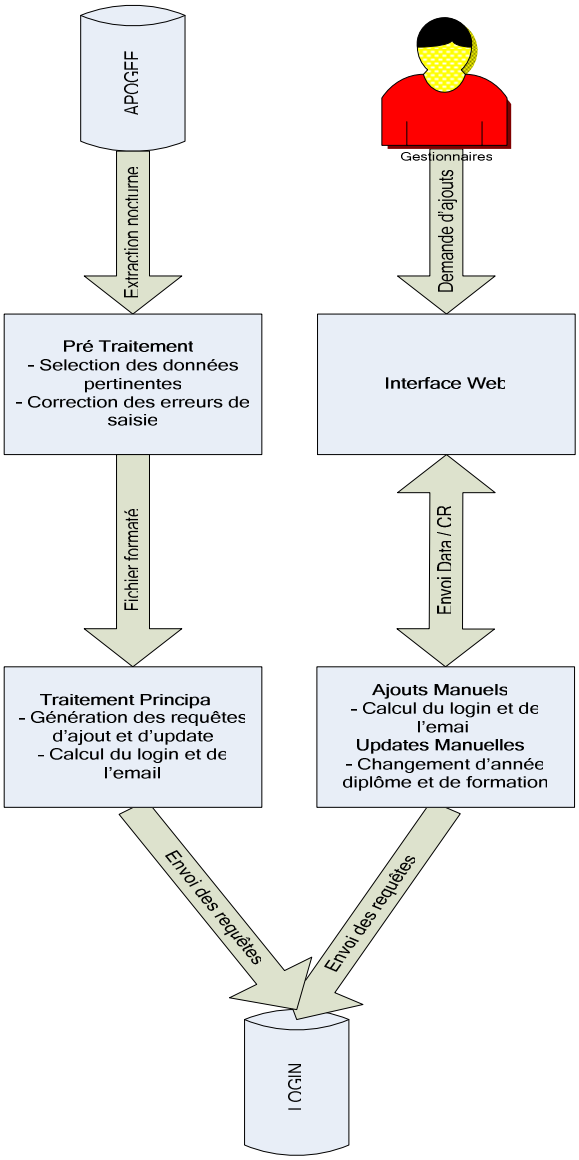

Figure 1 – *La création des entrées*

Depuis la rentrée 2005, nous demandons également de référencer l'UFR et le diplôme dans lequel l'étudiant est censé être inscrit. Cette contrainte supplémentaire a pour objectif de permettre l'établissement de l'annuaire LDAP et la mise en place des accès aux ressources spécifiques liées au portail ESUP.

2.5 La consultation des entrées

La base de données ainsi constituée est devenue le centre d'information principal pour les administrateurs systèmes ainsi que pour la génération des annuaires de l'Etablissement (Etumail, SUPANN, *Active Directory*).

La consultation de la base peut se faire par l'intermédiaire d'une application web que nous avons développée. Cette application offre aux administrateurs systèmes la possibilité de faire des recherches en utilisant les critères suivants :

- Nom
- Prénom
- Date de naissance
- Année diplôme
- UFR
- Formation

La recherche peut se faire de façon manuelle ou plus globalement en utilisant un fichier contenant le nom, le prénom et éventuellement la date de naissance des étudiants. Le résultat de la recherche est affiché dans une page web mais peut également être transmis par mail au demandeur.

Nous offrons aussi la possibilité aux administrateurs qui le souhaitent, d'effectuer directement des requêtes SQL (SELECT) sur la base.

Remarque : Afin d'améliorer les performances de la base celle-ci a été indexée sur les colonnes les plus utilisées.

2.6 La suppression des entrées

Lorsque nous supprimons une entrée dans la base de données, nous mettons en quarantaine le login et l'alias de messagerie électronique dans deux tables (*delogin* et *delmail*). Cette mise en quarantaine nous permet de ne pas réaffecter tout de suite un login ou une adresse de messagerie. La durée de cette quarantaine est actuellement de 18 mois.

Pour le cas particulier des ajouts manuels non régularisés, nous envoyons régulièrement un courrier électronique aux gestionnaires ayant créés ces entrées pour savoir si elles ont encore lieu d'être ou non. Si un ajout manuel doit disparaître, il est effacé sans délai.

2.7 Les avantages de la solution

Cette base de données, adaptée aux besoins des gestionnaires de comptes, offre plusieurs avantages.

Les principaux sont :

- Fourniture d'un login et d'un alias de messagerie unique pour tous les étudiants de l'université.
- Possibilité d'anticiper l'inscription des étudiants par des ajouts manuels.
- Mise à disposition des administrateurs.
- Simplicité et souplesse de la solution.

- Bibliothèque de fonctions PHP permettant de créer aisément des modules d'accès à la base.

2.8 Les inconvénients de la solution

Les inconvénients associés à la base de données sont surtout liés aux ajouts manuels. En effet, ces ajouts peuvent poser des problèmes de mise à jour dans le cas où il y a une différence entre les informations saisies par un gestionnaire (nom, prénom et date de naissance) et celles saisies par les services administratifs lors de l'inscription effective de l'étudiant. Si le triplet nom, prénom et date de naissance est différent, il y aura alors 2 lignes dans la base de données au lieu d'une.

Les autres inconvénients restent assez marginaux. Parmi ceux-ci, on peut citer :

- Etudiants étrangers ne possédant pas de prénom.
- Noms et prénoms composés très longs qui génèrent des alias de messagerie complexes.
- Etudiantes mariées…

2.9 La version actuelle

Jusqu'à présent, nous utilisions comme élément unique le triplet composé du nom, prénom et date de naissance de l'étudiant.

Pour récupérer ses identifiants, l'étudiant devait donner sa date de naissance et son numéro INE qui apparaissait sur la carte d'étudiant. Suite à la disparition de cette information sur les nouvelles cartes, nous avons intégré le numéro de dossier Apogée.

Nous l'utilisons lors des mises à jour (réinscriptions) et pour gérer les inscriptions multiples. Ce numéro de dossier invariant dans Apogée, nous permet de réduire le nombre d'erreurs liées aux problèmes de saisie générant des corrections dans Apogée (mauvaise date de naissance, faute d'orthographe du nom ou du prénom, …).

Nous avons également ajouté certains champs (le sexe de l'étudiant par exemple) afin de pouvoir prochainement générer l'annuaire SUPANN depuis la base LOGIN.

Dernièrement, nous proposons également de mettre à jour manuellement des lignes déjà présentes dans la base de données. Cette fonctionnalité permet de régler certains problèmes de réinscriptions tardives d'étudiants en les faisant passer dans l'année en cours. La ligne est alors considérée comme étant une entrée manuelle et devra donc être confirmée rapidement par une réinscription administrative de l'étudiant.

2.10 Le bilan

Cette base de données que nous utilisons depuis 5 ans a montré sa fiabilité et sa flexibilité. Les modifications nécessaires lors de l'avancement du projet ont été transparentes pour les utilisateurs.

La base s'est enrichie au cours des années et elle est devenue la source des annuaires utilisés dans l'Etablissement.

Elle alimente l'annuaire LDAP utilisé par l'application Etumail ainsi que l'annuaire *Active Directory* (ADUHP). L'alimentation de l'annuaire SUPANN est en projet.

Ces annuaires sont mis à jour directement par des requêtes SQL dans la base.

A ce moment du projet, nous disposons de la pierre angulaire nécessaire à la poursuite de notre objectif. Chaque étudiant dispose toujours de plusieurs comptes mais maintenant son login est unique. La mise en place d'un annuaire LDAP est maintenant possible.

3 L'annuaire LDAP

3.1 Introduction

La base LOGIN étant maintenant capable de fournir des informations uniques pour authentifier les étudiants, la mise à disposition d'un système de messagerie était la priorité définie par l'établissement. En effet, à cette époque, seule une minorité d'étudiants qui suit un cursus informatique dispose d'adresses électroniques.

Il a donc été décidé de mettre en place un service de messagerie qui s'appuie sur une authentification LDAP.

Cet annuaire LDAP est aussi nécessaire pour la mise en place des futurs services que l'établissement souhaite développer.

Comme nous l'avions décidé au début du projet, l'annuaire et le système de messagerie s'appuient sur du logiciel libre.

3.2 La solution de messagerie retenue

Le système de messagerie utilise courier-IMAP et postfix. Les fonctionnalités d'antivirus, *antispam*, *blacklists* et *greylists* ont également été implémentées.

Les clients de messagerie contactent le serveur (POP/POPS/IMAP/IMAPS) qui utilise l'authentification sur l'annuaire LDAP.

Un service de *webmail* (IMP) authentifiant aussi l'utilisateur sur l'annuaire est fourni aux étudiants.

3.3 La solution d'annuaire retenue

Le serveur LDAP utilisé est OpenLDAP.

Le schéma de l'annuaire LDAP est constitué des UFR pour le 1er niveau de hiérarchisation puis des diplômes pour le second.

L'annuaire est alimenté par la base LOGIN qui lui fournit un fichier contenant les créations et les modifications à apporter.

L'annuaire contient

- Les informations nécessaires au système de messagerie (adresse email, redirection de courrier, multi domaine de messagerie, les quotas….).
- Les informations propres à l'étudiant et à son inscription (nom, prénom, ufr, étape, ine, date de naissance) pour créer des listes de messagerie…
- Le login et le mot de passe de l'étudiant pour toute application qui souhaiterait baser son authentification sur l'annuaire.

Pour sécuriser les accès à l'annuaire, des Acls sont positionnés sur les attributs LDAP en fonction des besoins des applications.

3.4 La problématique de l'authentification

Dans la phase de mise à disposition des services, des choix ont été faits pour en faciliter l'implantation et le développement.

Le mot de passe initial est généré aléatoirement. Il est stocké crypté pour le processus d'authentification et sera modifié lorsque l'étudiant le changera.

De plus, le mot de passe initial est aussi conservé en clair dans l'annuaire afin de pouvoir le repositionner lorsque l'étudiant le perd. Cette solution n'est pas très "*sécure*", mais dans la phase de mise en place d'une messagerie aussi importante (17000 étudiants), c'était la plus simple pour résoudre le problème des pertes de mots de passe.

L'étudiant récupère son mot de passe initial et l'adresse électronique au travers d'une interface en donnant son numéro INE et sa date de naissance. Il peut aussi par l'interface, modifier son mot de passe et il dispose de l'accès à la messagerie, à un annuaire électronique par formation et à quelques informations.

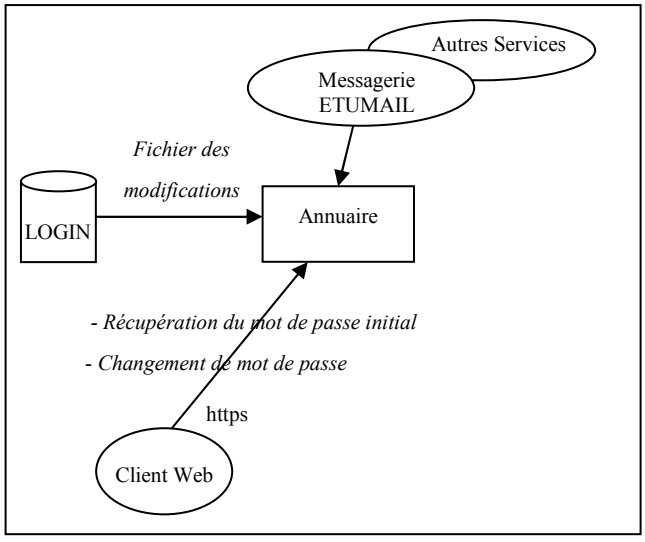

Figure 2 – *Etumail : Version iniale*

Il faut préciser aussi qu'à cette époque, dans certaines composantes, devant le manque de machines et le nombre important d'étudiants, le mot de passe initial et le login sont souvent fournis par les administrateurs ou un secrétariat.

Cette première mouture mise en place dans l'urgence présente des défauts et des manques qui ont été traités au fur et à mesure de l'avancement du projet.

3.5 La version actuelle

Nous nous sommes aperçus que la fourniture par LOGIN d'un fichier de modification n'était pas une solution évolutive et nous avons recadré les fonctions de chaque application.

- La base LOGIN a pour vocation **uniquement** de générer et contenir les informations utiles aux applications.
- L'annuaire LDAP (ou tout autre annuaire ou base) va chercher les informations directement dans la base LOGIN pour se mettre à jour.

Ce système est plus logique et beaucoup plus souple lorsque l'on fait évoluer chaque composant.

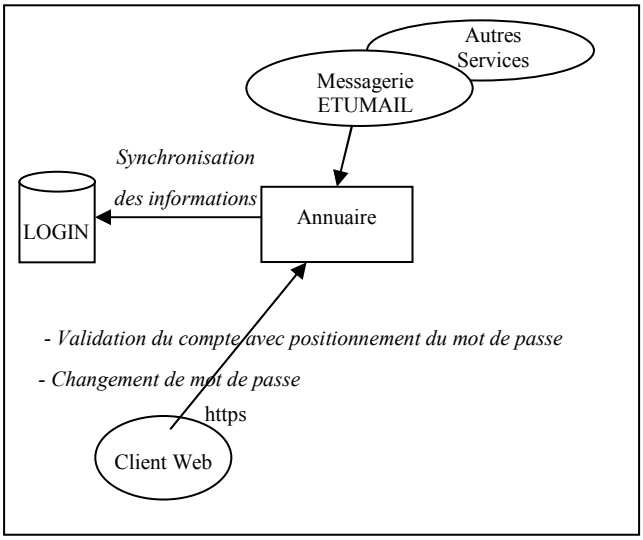

Figure 3 – *Etumail : Version actuelle*

L'annuaire LDAP s'est enrichi de nouveaux champs nécessaires à une meilleure gestion des mots de passe des étudiants. En effet, le stockage en clair du mot de passe initial et la diffusion par voie écrite devaient disparaître.

Les champs suivants ont été ajoutés :

- Le champ "valide" est renseigné lorsque l'étudiant valide son compte et dès que ce champ est renseigné, il n'est plus possible pour des raisons de sécurité de valider à nouveau le compte.
- Le champ "dossier Apogée" permet de valider un compte en utilisant le numéro de dossier Apogée en lieu et place du numéro INE qui n'est pas fiable à 100%.

La validation d'un compte repose entièrement sur la base LDAP et la validation par l'étudiant est obligatoire s'il veut accéder à son compte. Via l'interface, il positionne son mot de passe et il est maintenant le seul à le connaître.

3.6 Le bilan

Après la mise en place de la base LOGIN, l'annuaire LDAP était le passage obligé pour continuer le projet.

L'annuaire continue à s'enrichir en fonction des besoins des applicatifs et il est primordial pour le système de messagerie étudiante de l'établissement (ETUMAIL).

Dans cette première phase, nous disposons d'un système d'authentification centralisée pour l'ensemble des services web aux étudiants (ETUMAIL, annuaire, …) mais un étudiant a toujours plusieurs comptes pour accéder aux machines d'enseignement.

4 L'authentification Windows

4.1 Introduction

L'avancement du projet lorsque les étapes précédentes ont été opérationnelles, s'est trouvé bloqué par les spécificités et la rigidité du système propriétaire Windows…

Est il possible d'unifier l'authentification Windows sur un annuaire OpenLDAP ???

Nous avons testé ou fait tester dans le cadre de projets étudiants des solutions à base de Kerberos ou de pGina mais aucune de ces solutions ne nous a satisfait.

La solution kerberos n'est pas encore viable et la solution pGina fait perdre des fonctionnalités utiles à la gestion des comptes (droits d'accès, GPO, …).

Cette situation nous a conduit à choisir une étape intermédiaire en cherchant une solution qui permette de disposer d'une authentification unique dans le monde Windows, pour le monde Windows.

Cette opportunité s'est offerte à nous avec l'arrivée du système Windows 2000. Dans le cadre de la politique de formation de l'Université, une session d'une semaine a été financée pour tous les informaticiens qui le souhaitaient (mars 2003). Cette formation a été organisée par une société spécialisée dans le domaine. Elle a permis de former des administrateurs et d'appréhender les possibilités offertes par ce nouveau système.

Il est à noter que la plupart des administrateurs utilisaient déjà sur leur site un serveur Windows 2000 et que certains avaient réalisé des relations d'approbation entre leurs domaines pour essayer de résoudre les difficultés rencontrées par la gestion d'étudiants communs sur des matériels gérés indépendamment.

4.2 La solution retenue

Les solutions proposées par ce nouveau système nous ont amenés à réunir (avril 2003) toutes les personnes intéressées pour discuter de la possibilité de créer une forêt interconnectant les serveurs existants ou d'envisager la mise en place d'un mono domaine *Active Directory* couvrant toute l'Université.

La forêt, même si elle nous offrait une solution rassurante car elle ne remettait pas en cause les choix actuels de chaque administrateur, a été abandonnée très vite car elle ne nous offrait pas tous les services que nous attendions.

La solution de mettre en place un mono domaine (appelé **ADUHP**) a été longuement discutée car cette solution remettait en cause toute la gestion actuelle.

L'ampleur, l'ambition du projet et surtout la nécessité de partager les responsabilités avec d'autres administrateurs ont été les principales "peurs" exprimées. En effet, dans un mono domaine, toute modification est aussitôt répercutée sur l'ensemble des serveurs et peut provoquer une panne ou des problèmes sur tout ou partie du réseau.

La formation suivie par la majorité des personnes a permis à chacun de mesurer toute la problématique de ce mono domaine. La décision de mettre en place cette solution a été prise à la condition, qu'un cahier des charges et devoirs soit mis en place et que chacun s'engage à le respecter.

Le cahier des charges définit :

- Le rôle et la déontologie des administrateurs du domaine.
- L'uniformisation des noms des objets (GPO, groupes locaux, groupes globaux,…).
- Les choix des paramètres communs au domaine.
- La liste des OU (*Organization Unit*) communes ainsi que les OU des différents services.
- ….

Afin de sécuriser au mieux une telle architecture, le nombre d'administrateurs du domaine a été limité et ils ont été choisis parmi les personnes ayant suivi la formation. Il a été défini des OU principales afin que chaque entité puisse gérer en toute indépendance ses comptes (ordinateurs ou utilisateurs), ses groupes, ses GPO… Un profil d'administrateur d'OU a été défini afin que chacun puisse gérer les objets sous l'OU dont il est responsable. Un administrateur d'OU n'est donc pas obligé d'être administrateur du domaine pour gérer ses objets. Il a délégation sur son OU et uniquement sur son OU.

Une période de tests d'une année a été décidée pour appréhender l'ensemble des problèmes et des solutions à mettre en œuvre et ainsi aboutir à l'amélioration du cahier des charges et à la mise en production d'un *Active Directory* fiable. L'année universitaire 2003/2004 a vu le déploiement des différents serveurs et le rattachement de toutes les entités prêtes à participer à cette phase de tests.

En fait, la presque totalité des administrateurs s'est lancé dans l'aventure.

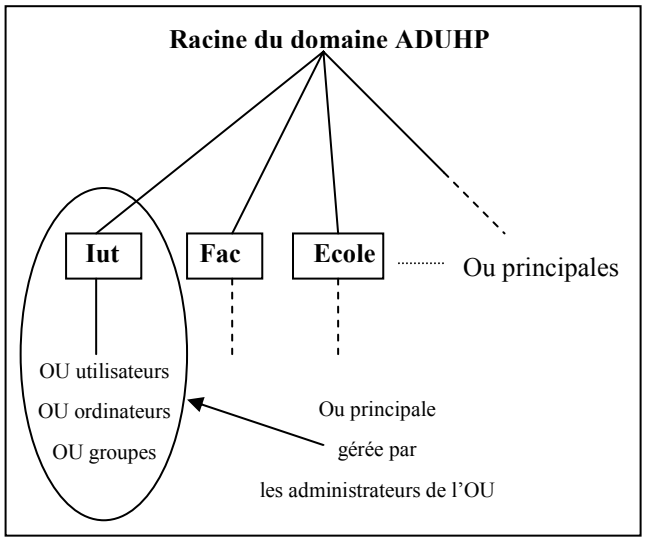

Figure 4 – *L'organisation du mono domaine*

4.3 Les avantages de la solution

Cette solution de disposer d'un mono domaine *Active Directory* apporte beaucoup d'avantages dans la gestion des comptes utilisateurs et facilite le travail des administrateurs.

Parmi les nombreux avantages, on peut citer :

- Un seul compte à créer et à gérer pour l'authentification sur tous les ordinateurs Windows de l'Université.
- Un étudiant peut avoir accès sous certaines conditions, à tous les ordinateurs de l'Université.
- La suppression des relations d'approbation entre les différents domaines AD.
- Le système de réplication qui transmet à tous les serveurs les modifications sur les objets.
- En cas de coupure réseau, chaque entité d'enseignement peut continuer à utiliser son serveur et toutes les modifications sont propagées dès la reprise du service réseau.
- La délégation de droits qui permet aux administrateurs d'OU de positionner des GPO limitées à l'OU et de gérer des groupes locaux et globaux.
- Les GPO et les groupes locaux permettent de limiter l'accès à des salles aux seules personnes autorisées.
- …

4.4 Les inconvénients de la solution

Cette solution comporte aussi quelques inconvénients qui sont rarement techniques mais plutôt humains.

Parmi les inconvénients, on peut citer :

- Moins de liberté pour les administrateurs par rapport à l'ancien fonctionnement et plus de responsabilités vis à vis de la communauté.
- Respect des contraintes de nommage.
- Respect du code de déontologie.
- Utilisation du serveur AD uniquement pour la gestion des comptes. Il est interdit pour des raisons de sécurité, d'installer des logiciels accessibles par l'extérieur (exemple : IIS) …

Le recul que nous avons sur le problème, nous conduit à penser que ce que nous avons considéré dans un premier temps comme des inconvénients, sont devenus des atouts pour assurer une cohésion et un esprit d'équipe entre tous les informaticiens de l'Université disséminés sur trois départements.

4.5 Le bilan

La configuration présentée est en production maintenant depuis deux années et donne entière satisfaction aux administrateurs systèmes.

Cette période de fonctionnement nous a permis d'acquérir de l'expérience et surtout de cibler les petites imperfections à rectifier. Lors de notre dernière réunion de travail (juin 2005), il a été décidé de modifier la gestion des comptes utilisateurs afin de permettre une gestion automatisée.

La nouvelle version est opérationnelle depuis la rentrée 2005.

4.6 La version actuelle

Dans la version de départ, les administrateurs créaient et géraient leurs utilisateurs et leurs groupes d'étudiants directement dans leurs propres OU.

L'arrivée du LMD et les difficultés rencontrées pour passer d'une année universitaire à une autre, nous ont conduits à modifier fortement notre premier modèle.

En effet, il a été décidé de stocker tous les comptes étudiants dans une seule OU ETUDIANT, tous les groupes globaux dans une seule OU GROUPE et de créer/modifier automatiquement les comptes à partir de la base des logins.

Les administrateurs utilisent maintenant les groupes globaux générés automatiquement pour configurer leurs groupes locaux.

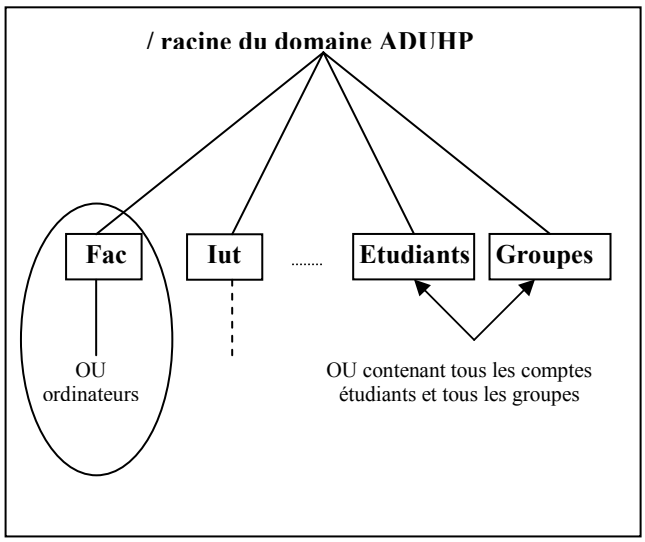

Figure 5 – *L'organisation actuelle*

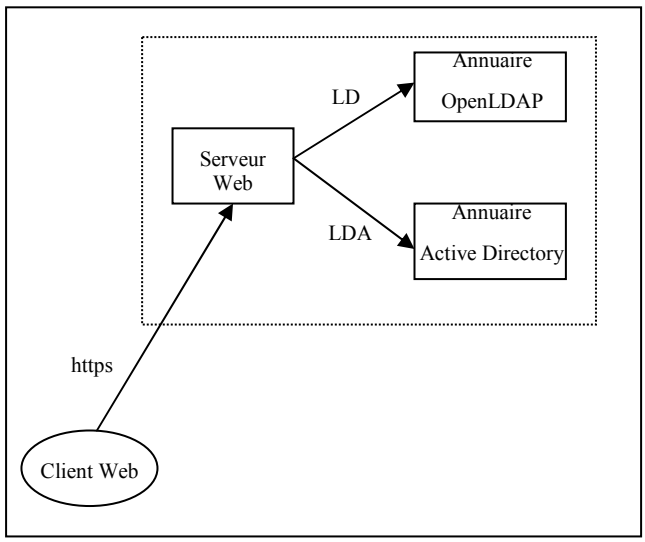

Figure 6 – Modification d'un mot de passe

Après cette étape, nous disposons pour chaque étudiant de deux comptes distincts qui se composent du même login mais dont les mots de passe peuvent être différents. Il nous reste donc à trouver une solution pour assurer l'unicité des mots de passe.

5 L'unification des mots de passe

5.1 Introduction

A ce niveau du projet, nous nous sommes donc retrouvés avec deux annuaires LDAP : OpenLDAP et *Active Directory*. Si nous avions beaucoup d'expérience dans la gestion d'un annuaire OpenLDAP via des scripts PHP, nous ne savions pas ce que l'annuaire LDAP de Microsoft nous permettait.

Après quelques tests d'accès à *Active Directory* par des scripts PHP, il a été rapidement évident que nous pouvions faire beaucoup de choses automatiquement dans cet annuaire. Cependant, tout n'est pas possible et la manipulation des mots de passe n'est pas triviale.

Une présentation au JRES 2003 (Michel Lastes – LIMSI Paris Sud) et une visite dans son laboratoire nous ont convaincus qu'il était possible de modifier un mot de passe et nous avons travaillé dans ce sens.

La réussite de nos tests nous a permis de développer une interface web qui réalise, après différentes vérifications, la modification des mots de passe sur les deux types d'annuaires simultanément.

Nous avons par GPO, interdit la modification de mot de passe directement sur un poste Windows et ainsi, la seule solution pour modifier un mot de passe est l'interface.

5.2 Le mot de passe Windows

Dans un annuaire OpenLDAP, le mot de passe peut être, au choix, stocké dans divers formats (crypt, md5,..) et peut être modifié facilement en utilisant un compte ayant les droits nécessaires sur le paramètre. Par contre, dans un annuaire *Active Directory*, le mot de passe est au format unicode et il ne peut être manipulé qu'en utilisant le protocole LDAPs.

Il est donc nécessaire d'utiliser un certificat pour pouvoir réaliser cette opération.

Actuellement, nous utilisons un certificat généré par le serveur principal du domaine ADUHP et nous allons faire des tests dans les prochaines semaines pour utiliser un certificat du CRU.

5.3 Le bilan

L'interface web actuellement disponible aux étudiants permet de valider leur compte lors de leur première inscription dans notre Université. En fournissant sa date de naissance, son numéro de dossier Apogée et le mot de passe à positionner, l'étudiant reçoit son login et son mot de passe est synchronisé sur ses comptes. Il doit aussi valider le fait qu'il accepte la charte informatique de l'Etablissement, sinon le compte n'est pas validé.

Il est de plus obligé de passer par l'interface s'il veut, par la suite, modifier son mot de passe.

Ce système est maintenant opérationnel depuis plus d'un an et aucun problème majeur n'est venu remettre en cause nos choix.

Nous disposons maintenant pour chaque étudiant d'un compte virtuel (sésame) composé de plusieurs comptes physiques mais qui disposent du même login et du même mot de passe.

6 La gestion des comptes

6.1 Introduction

Si la mise à jour du mot de passe était bloquante pour la poursuite du projet, ce n'est en fait qu'une petite pierre dans l'édifice que nous avons mis en place. De nombreux développements ont été faits pour déléguer en toute sécurité la gestion des comptes étudiants à des personnels non informaticiens.

L'interface web que nous avons développée a été conçue pour être utilisée par les étudiants et les personnels. Les différentes actions mises à disposition sont présentées en fonction du profil de l'utilisateur.

De plus, chaque action est un programme indépendant qu'il suffit de déclarer dans les fichiers de configuration pour qu'il soit instantanément intégré dans les profils autorisés.

Le nombre des actions possibles n'est dépendant que des besoins et de l'imagination des administrateurs.

6.2 Les gestionnaires

Dans notre stratégie globale, nous avons vu que le nombre de personnes disposant de droits administrateurs avait été volontairement restreint.

Or, dans une structure aussi importante, il est nécessaire que chacun puisse participer au bon fonctionnement quel que soit son statut ; ingénieurs, techniciens, secrétaires, personnels des bibliothèques, enseignants,… et l'utilisation d'une interface web nous permet de déléguer un ensemble d'actions sans que les personnes interviennent directement sur les serveurs.

Un système de profil a été développé pour particulariser les actions en fonction des besoins du gestionnaire.

Un gestionnaire suivant son profil peut :

- Créer un compte étudiant.
- Valider un compte étudiant (en sa présence).
- Changer un mot de passe étudiant (en sa présence).
- Chercher l'existence du compte d'un étudiant.
- Visualiser les paramètres du compte d'un étudiant.
- Créer des comptes ordinateurs
- …

Cette stratégie nous a permis de disposer d'un nombre très important de personnes capables de renseigner les étudiants en cas de problèmes et une bonne partie d'entre eux ne sont pas informaticiens.

La gestion a été déléguée au plus près des étudiants.

6.3 La création des comptes étudiants

Comme nous l'avons vu dans les paragraphes précédents, nous avons une gestion « presque » totalement automatisée des comptes étudiants, que ce soit dans l'annuaire OpenLDAP ou que ce soit dans l'annuaire *Active Directory* **ADUHP**.

Toute modification de la base Apogée (un étudiant change son inscription,…) est répercutée via la base LOGIN sur l'ensemble des annuaires.

Les seules interventions directes sur les comptes étudiants consistent actuellement à régler les inévitables cas particuliers qui apparaissent obligatoirement lorsque l'on traite 17000 comptes et à lancer le nettoyage des annuaires (destruction des comptes) conformément à la durée de vie des comptes telle qu'elle est prévue dans la charte informatique de l'Etablissement. Ces derniers points sont en cours de réflexion pour être automatisés.

Des programmes de vérification de cohérence entre les différentes bases et les différents annuaires (Apogée, LOGIN, OpenLDAP, *Active Directory*) sont lancés toutes les nuits et fournissent dans des fichiers journaux, les incohérences relevées.

6.4 Le cas de la Bibliothèque Universitaire

Il nous semble important de montrer par cet exemple que notre volonté a été de disposer d'un outil qui réponde à l'ensemble des besoins de notre Université.

En effet, la BU dont les trois sections sont intégrées dans le projet, présente la particularité d'ouvrir des accès à ses moyens documentaires à des personnes qui ne sont pas ou plus étudiants (médecins, dentistes,…). Ces personnes sont des lecteurs autorisés qui s'inscrivent et qui doivent pouvoir disposer d'un accès informatique.

Nous avons donc créé des actions personnalisées qui permettent aux bibliothécaires de créer dans l'annuaire ADUHP, les comptes liés aux lecteurs autorisés. Ils peuvent donc créer, détruire ou modifier ces comptes en toute indépendance et en toute sécurité.

6.5 Conclusion

La simplicité avec laquelle, il est possible d'ajouter de nouvelles actions, de nouveaux gestionnaires, de nouveaux profils et l'indépendance de fonctionnement des modules par rapport au fonctionnement de l'interface nous permet de répondre rapidement à tous les cas de figure qui peuvent se présenter.

7 Etat des lieux

Notre projet est déjà bien avancé et a atteint le premier objectif que nous nous étions fixés mais il reste encore beaucoup de travail pour améliorer et étendre la solution.

L'interface web a été cassifiée et est intégrée dans le portail (ESUP) de l'Etablissement.

La présence des deux annuaires LDAP (ETUMAIL et SUPANN), nécessaire au regard de la chronologie de notre projet, va faire l'objet d'une discussion pour juger de la pertinence de les fusionner.

Pour l'authentification des stations Unix, il nous faut valider la fiabilité des réplicats LDAP.

Le développement nécessaire à l'intégration dans le projet des sites délocalisés a été réalisé et doit être testé dans les semaines à venir.

Un grand nombre de modules à destination des gestionnaires est en projet….

Remerciements

Comme nous l'avons précisé, beaucoup de personnes ont apporté leur concours à ce projet. Nous tenons à remercier :

- Michel Lastes du LIMSI.
- Les JRES qui nous ont fait connaître le travail de Michel Lastes.
- Christian, Eric, Nicolas pour leur aide précieuse dans le développement des applications et la résolution de problèmes techniques.
- Alain pour sa connaissance d'Apogée et sa bonne humeur communicative.
- Jean-Marc et Sylvain pour la mise en œuvre de l'annuaire SUPANN.
- Sabine, Bruno, Christophe et bien d'autres qui ont cru au projet.
- Tous les personnels de l'Université qui ont permis le succès du déploiement auprès des étudiants….

S Y N O P T I Q U E G L O B A L D E L A S O L U T I O N